UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/561,896	12/21/2005	Gerardus T.M. Hubert	GB030098US1	1091

65913   7590   11/14/2008

NXP, B.V.
NXP INTELLECTUAL PROPERTY DEPARTMENT
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER
NGUYEN, TRONG H

ART UNIT	PAPER NUMBER
4148	

NOTIFICATION DATE	DELIVERY MODE
11/14/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Office Action Summary

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 December 2005*.
2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.
     4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) *1-33* is/are rejected.
7)☒ Claim(s) *1,5,13-15,18,22,27 and 28* is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on *21 December 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
     a)☒ All   b)☐ Some *   c)☐ None of:
        1.☒ Certified copies of the priority documents have been received.
        2.☐ Certified copies of the priority documents have been received in Application No. _____.
        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
     * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
     Paper No(s)/Mail Date *12/21/2005*.

4) ☐ Interview Summary (PTO-413)
     Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____ .

DETAILED ACTION

1.   The instant application numbered 10561896 filed on 12/21/2005 is presented for examination by the examiner.

Oath/Declaration

2.   The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in 37 C.F.R. 1.63.

Priority

3.   As required by M.P.E.P. 201.14(c), acknowledgement is made of applicant's claim for priority based on application filed on 06/21/2003 (GB 0314557.0).

4.   Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Drawings

5.   The applicant's submitted drawings are acceptable for examination purposes.

Information Disclosure Statement

6.   The information disclosure statement (IDS) submitted on 12/21/2005 is in compliance with the provisions of 37 C.R.R. 1.97.   Accordingly, the information disclosure statement is being considered by the examiner.

Specification

7.   Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

8.   The abstract of the disclosure is objected to because the abstract is less than the minimum 50 word limit, not in narrative form, and not much descriptive in describing the disclosure. Correction is required. See MPEP § 608.01(b).

9.   The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: Reduction calculations in Elliptic Curve Cryptography.

10.   The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.

(f) BACKGROUND OF THE INVENTION.
    (1) Field of the Invention.
    (2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

11.   The disclosure is objected to because of the following informalities: Important variables used in the specification such as N, B, n_0, R, n_0', or m, etc. should be carefully defined as to provide a clear understanding of the claimed invention. Appropriate correction is required.

Claim Objections

12.   Claim **1** is objected to because of the following informalities: line 3 recites "8ignificant" which appears to be a misspelling of "significant". Appropriate correction is required.

13.   Claims **1, 5, 18, and 22** are objected to because of the following informalities:
last lines of these claims recite "multiple" which appears to be referred to "multiple of a
modulus" and hence is inconsistent. Appropriate correction is required.

14.   Claim **13** is objected to because of the following informalities: line 2 recites
"ECG" which appears to be a misspelling of "ECC". Appropriate correction is required.

15.   Claim **17** is objected to under 37 CFR 1.75(c) as being in improper form because
a multiple dependent claim should refer to other claims in the alternative only--, and/or, -
-cannot depend from any other multiple dependent claim. See MPEP § 608.01(n).
Accordingly, the claim has not been further treated on the merits.

16.   Claim **22** is objected to because of the following informalities: line 2 recites "(10-
17)" which should be omitted. Appropriate correction is required.

17.   Claim **27** is objected to because of the following informalities: last line recites
"(K-2)" which appears to be referred to (k-2) and thus is inconsistent. Appropriate
correction is required.

18.   Claim **28** is objected to because of the following informalities: line 2 recites
"EEC" which appears to be a misspelling of "ECC". Appropriate correction is required.

Claim Rejections - 35 USC § 112

19.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

       Claims **1** and **18** recite the limitation "the number" in line 4. There is insufficient
antecedent basis for this limitation in these claims.

Claims **6** and **23** recite "the last multiplication" in line 2 and "the selected number" in last line. There is insufficient antecedent basis for these limitations in these claims. Furthermore, it is unclear as which number the applicant was referring to by "the selected number". For examining purposes, hereinafter "the selected number" will be considered as an intermediate result or result from a multiplication process.

Claims **7** and **24** recite "n_0'" in line 2 and last line respectively. Even though n_0' was defined in the specification as equal to $B-n_0$ on page 5 line 14, none of the parameters such as B and n_0 and other pertinent parameters identified in the specification are introduced or have any antecedent basis in these claims or their parent claims. Therefore, there is insufficient antecedent basis for this limitation in these claims.

Claims **8** and **25** recite "the carry c" in line 2 and "the addend" in last line. There is insufficient antecedent basis for these limitations in these claims.

Claims **9** and **26** recite "the number" in last line. There is insufficient antecedent basis for these limitations in these claims.

Claims **9-10** and **26-27** recite "(k-2)" in last lines. Even though k was mentioned in the specification, it is not introduced nor has any antecedent basis in these claims or their parent claims. Therefore, there is insufficient antecedent basis for this limitation in these claims. For examining purposes, hereinafter, (k-2) will be considered as any positive number.

Claims **10** and **27** recite "the next calculation" and "the number" in last line. There is insufficient antecedent basis for these limitations in these claims.

Claim **21** recites "the combined multiplication operations and reduction operation" in lines 2-3. There is insufficient antecedent basis for this limitation in the claim.

Claim **30** recites "Apparatus according to claim 18 with means for 256-bit ECC and 81 word size of 64-bit, the modulus comprises 81 first section of 202 bits and 81 second section of 54 bits" in lines 1-3. Since 81 word size of 64 bits is even larger than 256-bit ECC, it is unclear as to what the applicant meant. For examining purposes, hereinafter "81 word size of 64-bit", "81 first section of 202 bits" and "81 second section of 54 bits" will be considered as "a word size of 64-bit", "a first section of 202 bits" and "a second section of 54 bits".

Claim **31** recites "A method of performing a reduction operation substantially as hereinbefore described with reference to, and/or as illustrated in, anyone or more of Figures 1 to 5 of the accompanying drawings" in lines 1-3. It is unclear as to what the meets and bounds of the claimed invention are. For examining purposes, hereinafter, this method will be considered as the same method described in claim **1**.

Claim **32** recites " A method of performing a reduction operation substantially as hereinbefore described with reference to, and/or as illustrated in, anyone or more of Figures 1 to 5 of the accompanying drawings" in lines 1-4. It is unclear as to what the meets and bounds of the claimed invention are. For examining purposes, hereinafter, this method will be considered as the same method described in claim **1**.

Claim **33** recites " A method of performing a reduction operation substantially as hereinbefore described with reference to, and/or as illustrated in, anyone or more of Figures 1 to 5 of the accompanying drawings" in lines 1-4. It is unclear as to what the

meets and bounds of the claimed invention are. For examining purposes, hereinafter, this method will be considered as the same method described in claim **1**.

Claim Rejections - 35 USC § 101

20.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims **1-33** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter because of the following reasons:

Claims **1**, **18 and 31-33** are directed to a method and apparatus for performing a mathematical function without transforming an article or physical object to a different state or thing or producing a useful, concrete, and tangible result. In order to be statutory, claims must include a practical application with a useful, concrete and tangible result. However, it is clear from independent claims **1**, **18**, and **31-33** that the claimed invention merely involves calculations and manipulations of data without disclosing a practical application with a useful, concrete and tangible result. Thus, independent claims **1**, **18**, and **31-33** are directed to non-statutory subject matter.

Claims **2-17** and **19-30** are rejected for similar reasons as discussed for their respective parent claims, as they fail to present any limitations that resolve the deficiencies of the claims from which they depend.

Claim **14** is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter of software, *per se*. The claim lacks the

necessary physical articles or objects to constitute a machine or manufacture within the meaning of 35 U.S.C. 101. It is clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. It is at best, function descriptive material *per se*.

Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." Both types of "descriptive material" are non-statutory when claimed as descriptive material *per se*, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994).

Merely claiming non-functional descriptive material, i.e., abstract ideas, stored on a computer-readable medium, in a computer, or on an electromagnetic carrier signal, does not make it statutory. See *Diehr*, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in *Benson* were unpatentable as abstract ideas because "[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer.").

In this case, applicant has claimed a "a computer program product" in claim **14** to be run on a computer; this implies that applicant is claiming a system of software, per se, lacking the hardware necessary to realize any of the underlying functionality.

Therefore, claim **14** is directed to non-statutory subject matter as computer programs, per se, i.e. the descriptions or expressions of the programs, are not physical "things." They are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed elements of a computer, which permit the computer program's functionality to be realized.

Claim **17** is rejected under 35 U.S.C. 101 as non-statutory for at least the reason stated above. Claim **17** is depended on claim **14**, however, it does not add any feature or subject matter that would solve any of the non-statutory deficiencies of claim **14**.

Claim **15** is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter of software, *per se*. The claim lacks the necessary physical articles or objects to constitute a machine or manufacture within the meaning of 35 U.S.C. 101. It is clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. It is at best, function descriptive material *per se*.

Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." Both types of "descriptive material" are non-statutory when claimed as descriptive material *per se*, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive

material to be realized. Compare *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994).

Merely claiming non-functional descriptive material, i.e., abstract ideas, stored on a computer-readable medium, in a computer, or on an electromagnetic carrier signal, does not make it statutory. See *Diehr*, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in *Benson* were unpatentable as abstract ideas because "[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer.").

In this case, applicant has claimed a "a computer program" in claim **15** to be run on a computer; this implies that applicant is claiming a system of software, per se, lacking the hardware necessary to realize any of the underlying functionality. Therefore, claim **15** is directed to non-statutory subject matter as computer programs, per se, i.e. the descriptions or expressions of the programs, are not physical "things." They are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed elements of a computer, which permit the computer program's functionality to be realized.

Claim **16** is rejected under 35 U.S.C. 101 as non-statutory for at least the reason stated above. Claim **16** is depended on claim **15**, however, it does not add any feature or subject matter that would solve any of the non-statutory deficiencies of claim **15**.

Claims **16-17** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter because of the following reason:

Regarding claim **16**, the claim fails to place the invention squarely within one statutory class of invention. In line 1 of the claim, applicant claimed "a carrier, which may comprise electronic signals". As such, the claim is drawn to a form of energy. Energy is not one of the four categories of invention and therefore this claim(s) is/are not statutory. Energy is not a series of steps or acts and thus is not a process. Energy is not a physical article or object and as such is not a machine or manufacture. Energy is not a combination of substances and therefore not a composition of matter. Hence, it is directed to non-statutory subject matter.

Regarding claim **17**, the claim fails to place the invention squarely within one statutory class of invention. Line 1 of the claim recites "electronic distribution" which is not one of the four categories of patent eligible subject matter recited in 35 U.S.C. 101 (process, machine, manufacture, or composition of matter); is not directed to a judicial exception to 35 U.S.C. 101 (i.e., an abstract idea, natural phenomenon, or law of nature) and it is not directed to a practical application of such judicial exception (e.g., because the claim does not require any physical transformation and the invention as claimed does not produce a useful, concrete, and tangible result). Hence, it is directed to non-statutory subject matter.

Claim Rejections - 35 USC § 102

21.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims **1-5, 14-22** and **31-33** are rejected under 35 U.S.C. 102(b) as being anticipated by Hollmann et al US 6,366,673 (hereinafter "Hollmann").

Regarding claim **1**, Hollmann discloses "**A method of performing a reduction operation in a cryptographic calculation,**" as [modified Quisquater method (Col. 5, line 16)] "**the method comprising selecting a modulus having a first section with a plurality of "1" Most significant Word states and a second section which comprises a, plurality of "1" or "0" states**" as [first p most significant bits of N are all equal to 1 (first section) and (n-p) bits may be "1" or "0" states (second section) (Col. 4, lines 3-4)] "**whereby the number formed of the two sections is a modulus or a multiple of a modulus,**" as [N is a multiple of modulus M (Col. 4, lines 3-4 and Col. 5, lines 17-18)] "**and operating a reduction operation on the modulus/multiple**" as [calculating z in inner loop (Col. 9, line 18 and Col. 9, lines 65-66)].

Regarding claim **2**, Hollmann discloses "**A method according to claim 1 comprising effecting a plurality of multiplication operations**" as [calculating h in inner loop (Col. 9, line 17 and Col. 9, lines 65-66)].

Regarding claim **3**, Hollmann discloses "**A method according to claim 2 comprising effecting a plurality of multiplication operations followed by effecting a reduction operation**" as [h calculations are followed by z calculations (Col. 9, line 17-18 and Col. 9, lines 65-66)].

Regarding claim **4**, Hollmann discloses "**A method according to claim 3 comprising repeating the combined multiplication operations and reduction**

operation" as [h and z calculations are repeated (Col. 9, line 16-18 and Col. 9, lines

65-66)].

Regarding claim **5**, Hollmann discloses **"A method according to claim 1**

comprising using a multiple of the modulus/multiple" as [all intermediate

computations are done modulo N instead of modulo M where N is a multiplicity of M

(Col. 5, lines 21-22)].

Regarding claim **14**, Hollmann discloses **"A computer program product**

directly loadable into the internal memory of a digital computer, comprising

software code portions for performing the method of claim 1 when said product is

run on a computer" as [As indicated in Hollmann's figures 1 and 2, the method of claim

1 is implemented in a computer system which inherently includes a software that

performs the intended method. Also, see rejection of claim **1** for rejection of the

method].

Regarding claim **15**, Hollmann discloses **"A computer program directly load**

able into the internal memory of a digital computer, comprising software code

portions for performing the method of claim 1 when said program is run on a

computer" as [As indicated in Hollmann's figures 1 and 2, the method of claim **1** is

implemented in a computer system which inherently includes a software that performs

the intended method. Also, see rejection of claim **1** for rejection of the method].

Regarding claim **16**, Hollmann discloses **"A carrier, which may comprise**

electronic signals, for a computer program of claim 15" as [As indicated in

Hollmann's figures 1 and 2, the method of claim **1** is implemented in a computer system

which inherently includes a software and a carrier for performing the intended method. Also, see rejection of claim **1** for rejection of the method].

Regarding claim **18**, Hollmann discloses "**Apparatus for performing a reduction operation in a cryptographic calculation,**" as [device for performing a reduction operation (Fig. 1, Col. 7, line 57)] "**the apparatus comprising means to select a modulus or a multiple of a modulus having a first section with a plurality of "1" states and a second section having a plurality of "1" or "0" states**" as [first p most significant bits of N are all equal to 1 (first section) and (n-p) bits may be "1" or "0" states (second section) (Col. 4, lines 3-4)] "**whereby the number formed of the two sections is a modulus or a multiple of a modulus,**" as [N is a multiple of modulus M (Col. 4, lines 3-4 and Col. 5, lines 17-18)] "**and means for operating a reduction operation on the modulus/multiple**" as [calculating z in inner loop (Col. 9, line 18 and Col. 9, lines 65-66)].

Regarding claim **19**, Hollmann discloses "**Apparatus according to claim 18 comprising means to effect a plurality of multiplication operations**" as [calculating h in inner loop (Col. 9, line 17 and Col. 9, lines 65-66)].

Regarding claim **20**, Hollmann discloses "**Apparatus according to claim 19 comprising means to effect a plurality of multiplication operations followed by a reduction operation**" as [h calculations are followed by z calculations (Col. 9, line 17-18 and Col. 9, lines 65-66)].

Regarding claim **21**, Hollmann discloses "**Apparatus according to claim 20 comprising means to repeat the combined multiplication operations and**

reduction operation" as [h and z calculations are repeated (Col. 9, line 16-18 and Col. 9, lines 65-66)].

Regarding claim **22**, Hollmann discloses "**Apparatus according to claim 18 comprising means (10-17) to use a multiple of the modulus/multiple**" as [all intermediate computations are done modulo N instead of modulo M where N is a multiplicity of M (Col. 5, lines 21-22)].

Regarding claim **31**, Hollmann discloses "**A method of performing a reduction operation substantially as hereinbefore described with reference to, and/or as illustrated in, anyone or more of FIGS. 1 to 5 of the accompanying drawings**" [As indicated in *Claim Rejections - 35 USC § 112* above, the meets and bounds of the claim are not clearly determined, therefore it is interpreted that the method is directed to the same method of claim **1** and rejected accordingly. See rejection of claim **1**].

Regarding claim **32**, Hollmann discloses "**Apparatus for performing a reduction operation in a cryptographic calculation, the apparatus substantially as hereinbefore described with reference to, and/or as illustrated in, anyone or more of FIGS. 1 to 5 of the accompanying drawings**" as [As indicated in *Claim Rejections - 35 USC § 112* above, the meets and bounds of the claim are not clearly determined, therefore it is interpreted that the apparatus is directed to the same apparatus of claim **18** and rejected accordingly. See rejection of claim **18**].

Regarding claim **33**, Hollmann discloses "**A method of performing a reduction operation in a cryptographic calculation, the method substantially as hereinbefore described with reference to, and/or as illustrated in, anyone or more**

of FIGS. 1 to 5 of the accompanying drawings" as [As indicated in *Claim Rejections*

- 35 USC § 112 above, the meets and bounds of the claim are not clearly determined,

therefore it is interpreted that the method is directed to the same method of claim **1** and

rejected accordingly. See rejection of claim **1**].

Claim Rejections - 35 USC § 103

22.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

23.   Claims **6-7** and **23-24** are rejected under 35 U.S.C. 103(a) as being unpatentable

over Hollmann in view of Blaker US 2002/0010730 (hereinafter "Blaker").

Regarding claim **6**, Hollmann discloses "**A method according to claim 1**" but

does not specifically disclose "**wherein, when the last multiplication gives an**

overflow, the overflow is added to a part of the selected number."

However, Blaker discloses adding an overflow bit to an intermediate result of a

multiplication operation (Col. 4, Par. 0036, lines 5-6).

Blaker and Hollmann are analogous art because they are in the same field of

endeavor of cryptology and computer arithmetic.

It would have been obvious to a person of ordinary skill in the art at the time of

the invention to modify Hollmann's modified Quisquater method by applying the

concept of adding the overflow bit to an intermediate result as described by Blaker since it would provide for the purpose of reducing latency in a multiplication process (Blaker, Col. 4, Par. 0036, line 9). Note that as indicated in the rejection of claim **6** under *Claim Rejections - 35 USC § 112* above, "the selected number" is considered as an intermediate result or result from a multiplication process.

Regarding claim **7**, Hollmann in view of Blaker disclose "**A method according to claim 6 wherein, when the overflow addition step produces an overflow, then n_0' is added to the overflow**" as [According to the multiplication criteria shown to be obvious in rejection of claim **1**, n_0' or its multiplicity is to be added to a selected number regardless of whether there exists an overflow or not. Claim **6**, which is depended on claim **1**, discusses the case when there is an overflow and the overflow is added to the selected number. Therefore, as indicated in the rejections of claim **6** and **1** above, it would be obvious to add n_0' (with multiplicity of 1) and the overflow to the selected number].

Regarding claim **23**, Hollmann discloses "**Apparatus according to claim 18**" but does not specifically disclose "**comprising means, when the last multiplication gives an overflow, to add the overflow to a part of the selected number.**"

However, Blaker discloses adding an overflow bit to an intermediate result of a multiplication operation (Col. 4, Par. 0036, lines 5-6).

Blaker and Hollmann are analogous art because they are in the same field of endeavor of cryptology and computer arithmetic.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's device by applying the concept of adding the overflow bit to an intermediate result as described by Blaker since it would provide for the purpose of reducing latency in a multiplication process (Blaker, Col. 4, Par. 0036, line 9). Note that as indicated in the rejection of claim **23** under *Claim Rejections - 35 USC § 112* above, "the selected number" is considered as an intermediate result or result from a multiplication process.

Regarding claim **24**, Hollmann in view of Blaker disclose "**Apparatus according to claim 23 comprising means, when the overflow addition step produces an overflow, to add n_0' to the overflow**" as [According to the multiplication criteria shown to be obvious in rejection of claim **18**, n_0' or its multiplicity is to be added to a selected number regardless of whether there exists an overflow or not. Claim **23**, which is depended on claim **18,** discusses the case when there is an overflow and the overflow is added to the selected number. Therefore, as indicated in the rejections of claim **23** and **18** above, it would be obvious to add n_0' (with multiplicity of 1) and the overflow to the selected number].

24.   Claims **8-9 and 25-27** are rejected under 35 U.S.C. 103(a) as being unpatentable over Hollmann in view of McGregor US 6,240,436 (hereinafter "McGregor").

Regarding claim **8**, Hollmann discloses "**A method according to claim 1**," but does not specifically disclose "**wherein the carry c between two adjacent multiplications is effected as the addend in the next multiplication.**"

However, McGregor discloses a Montgomery multiplication wherein a carry between two adjacent multiplications is added to the product of the next multiplication (Col. 8, lines 48-54).

Hollmann and McGregor are analogous art because they are in the same field of endeavor of cryptology and modular reduction.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's modified Quisquater method by applying the concept of using the carry between two adjacent multiplications as the addend in the next multiplication as described by McGregor since it would provide for the purpose of high-speed modular reductions given fixed processor operand capacities (McGregor, Col. 2, lines 40-41 and 48).

Regarding claim **9**, Hollmann discloses **"A method according to claim 1"** but does not specifically disclose "**comprising monitoring the number of leading "1"s to determine if the number is less than (k-2)**."

However, McGregor discloses a technique for monitoring the number of leading "1"s by shifting a window of a chosen size (Col. 6, lines 25-29).

Hollmann and McGregor are analogous art because they are in the same field of endeavor of cryptology and modular reduction.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's modified Quisquater method by using a window of a chosen size to monitor the number of leading "1"s and determine if the number is less than or greater than any certain positive number as described by McGregor since it

would provide for the purpose of reducing the number of multiplications necessary to perform an operation (McGregor, Col. 6, lines 3-4). Note that as indicated in the rejection of claim **9** under **Claim Rejections - 35 USC § 112** above, (k-2) is interpreted as any positive number.

Regarding claim **25**, Hollmann discloses "**Apparatus according to claim 18**" but does not specifically disclose "**comprising means to effect the carry c between two adjacent multiplications as the addend in the next multiplication.**"

However, McGregor discloses a Montgomery multiplication wherein a carry between two adjacent multiplications is added to the product of the next multiplication (Col. 8, lines 48-54).

Hollmann and McGregor are analogous art because they are in the same field of endeavor of cryptology and modular reduction.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's device by applying the concept of using the carry between two adjacent multiplications as the addend in the next multiplication as described by McGregor since it would provide for the purpose of high-speed modular reductions given fixed processor operand capacities (McGregor, Col. 2, lines 40-41 and 48).

Regarding claim **26**, Hollmann discloses "**Apparatus according to claim 18**" but does not specifically disclose "**comprising means to monitor the number of leading "1"s to determine if the number is less than (k-2).**"

However, McGregor discloses a technique for monitoring the number of leading "1"s by shifting a window of a chosen size (Col. 6, lines 25-29).

Hollmann and McGregor are analogous art because they are in the same field of endeavor of cryptology and modular reduction.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's device by using a window of a chosen size to monitor the number of leading "1"s and determine the if the number is less than or greater than a certain positive number as described by McGregor since it would provide for the purpose of reducing the number of multiplications necessary to perform an operation (McGregor, Col. 6, lines 3-4). Note that as indicated in the rejection of claim **26** under **Claim Rejections - 35 USC § 112** above, (k-2) is interpreted as any positive number.

Regarding claim **27**, Hollmann discloses "**Apparatus according to claim 18**" but does not specifically disclose "**comprising means to initiate the next calculation when the number of leading "1"s is less than (K-2).**"

However, McGregor discloses after detecting a leading "1", a multiplication operation is initiated (Col. 6, lines 44-45).

Hollmann and McGregor are analogous art because they are in the same field of endeavor of cryptology and modular reduction.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's device by initiating a next calculation when the number of leading "1"s is less than or greater than a certain positive number as

described by McGregor since it would provide for the purpose of reducing the number

of multiplications necessary to perform an operation (McGregor, Col. 6, lines 3-4).

Note that as indicated in the rejection of claim **27** under ***Claim Rejections - 35 USC §***

112 above, (k-2) is interpreted as any positive number.

25.   Claim **10** is rejected under 35 U.S.C. 103(a) as being unpatentable over

Hollmann in view of Blaker and further in view of McGregor.

Regarding claim **10**, Hollmann in view of Blaker discloses "**A method according**

to claim 6" but does not specifically disclose "**comprising initiating the next**

calculation when the number of leading "1"s is less than (k-2)."

However, McGregor discloses after detecting a leading "1", a multiplication

operation is initiated (Col. 6, lines 44-45).

McGregor, Hollmann, and Blaker are analogous art because they are in the

same field of endeavor of cryptology.

It would have been obvious to a person of ordinary skill in the art at the time of

the invention to modify the modified Quisquater method of Hollmann in view of Blaker

by initiating a next calculation when the number of leading "1"s is less than or greater

than a certain positive number as described by McGregor since it would provide for the

purpose of reducing the number of multiplications necessary to perform an operation

(McGregor, Col. 6, lines 3-4). Note that as indicated in the rejection of claim **10** under

Claim Rejections - 35 USC § 112 above, (k-2) is interpreted as any positive number.

26.   Claims **11-13 and 28-30** are rejected under 35 U.S.C. 103(a) as being unpatentable over Hollmann in view of Lenstra et al., Selecting Cryptographic Key Sizes, Journal of Cryptology, 14 August 2001 (hereinafter "Lenstra").

Regarding claim **11**, Hollmann discloses "**A method according to claim 1**" but does not specifically disclose "**the method comprising operating 192-bit ECC and a word size of 64-bit, the modulus comprises a first section of 138 bits and a second section of 54 bits**."

However, Lenstra discloses key size of 192 bits and word size of 64 bits are well known in cryptosystems and the key size and block size can vary (page 6, sec 2.2.1, lines 5-13). Furthermore, a modulus with a first section of 138 bits and a second section of 54 bits is an example of a combination of bits that is selected for an ECC operation. Thus, barring any unexpected result from particular selection of 192-bit ECC, 64-bit word size, modulus with a first section of 138 bits and a second section of 54 bits, it would have been obvious to select those particular numbers.

Lenstra and Hollmann are analogous art because they are in the same field of endeavor of cryptology.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's modified Quisquater method by selecting sections of a modulus to be of certain sizes and the key size and the word size as described by Lenstra since they are parameters that were used in the best-known cryptosystems (Lenstra, page 260, section 2.2.1, lines 5-6).

Regarding claim **12**, Hollmann discloses "**A method according to claim 1**" but does not specifically disclose "**the method comprises operating 128-bit ECC and a word size of 64-bit, the modulus comprises a first section of 74 bits and a second section of 54 bits.**"

However, Lenstra disclose key size of 128 bits and word size of 64 bits are well known in cryptosystems and the key size and block size can vary (page 260, sec 2.2.1, lines 5-13). Furthermore, a modulus with a first section of 74 bits and a second section of 54 bits is an example of a combination of bits that is selected for an ECC operation. Thus, barring any unexpected result from particular selection of 128-bit ECC, 64-bit word size, modulus with a first section of 74 bits and a second section of 54 bits, it would have been obvious to select those particular numbers.

Lenstra and Hollmann are analogous art because they are in the same field of endeavor of cryptology.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's modified Quisquater method by selecting sections of a modulus to be of certain sizes and the key size and the word size as described by Lenstra since they are parameters that were used in the best-known cryptosystems (Lenstra, page 260, section 2.2.1, lines 5-6).

Regarding claim **13**, Hollmann discloses "**A method according to claim 1**" but does not specifically disclose "**the method comprising operating 256-bit ECG and a word size of 54-bit, the modulus comprises a first section of 202 bits and a second section of 54 bits.**"

However, Lenstra disclose key size of 256 bits and word size of 64 bits are well known in cryptosystems and the key size and block size can vary (page 260, sec 2.2.1, lines 5-13). Furthermore, a modulus with a first section of 202 bits and a second section of 54 bits is an example of a combination of bits that is selected for an ECC operation. Thus, barring any unexpected result from particular selection of 256-bit ECC, 54-bit word size, modulus with a first section of 202 bits and a second section of 54 bits, it would have been obvious to select those particular numbers.

Lenstra and Hollmann are analogous art because they are in the same field of endeavor of cryptology.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's modified Quisquater method by selecting sections of a modulus to be of certain sizes and the key size and the word size as described by Lenstra since they are parameters that were used in the best-known cryptosystems (Lenstra, page 260, section 2.2.1, lines 5-6).

Regarding claim **28**, Hollmann discloses "**Apparatus according to claim 18**" but does not specifically disclose "**with means for 192-bit EEC and a word size of 64-bit, the modulus comprises a first section of 74 bits and a second section of 54 bits.**"

However, Lenstra disclose key size of 192 bits and word size of 64 bits are well known in cryptosystems and the key size and block size can vary (page 260, sec 2.2.1, lines 5-13). Furthermore, a modulus with a first section of 74 bits and a second section of 54 bits is an example of a combination of bits that is selected for an ECC operation. Thus, barring any unexpected result from particular selection of 192-bit ECC, 64-bit

word size, modulus with a first section of 74 bits and a second section of 54 bits, it

would have been obvious to select those particular numbers.

Lenstra and Hollmann are analogous art because they are in the same field of

endeavor of cryptology.

It would have been obvious to a person of ordinary skill in the art at the time of

the invention to modify Hollmann's device by selecting sections of a modulus to be of

certain sizes and the key size and the word size as described by Lenstra since they are

parameters that were used in the best-known cryptosystems (Lenstra, page 260,

section 2.2.1, lines 5-6).

Regarding claim **29**, Hollmann discloses "**Apparatus according to claim 18**" but

does not specifically disclose "**with means for 128-bit ECC and a word size of 64-bit,**

the modulus comprises a first section of 74 bits and a second section of 54 bits."

However, Lenstra disclose key size of 128 bits and word size of 64 bits are well

known in cryptosystems and the key size and block size can vary (page 260, sec 2.2.1,

lines 5-13). Furthermore, a modulus with a first section of 74 bits and a second section

of 54 bits is an example of a combination of bits that is selected for an ECC operation.

Thus, barring any unexpected result from particular selection of 128-bit ECC, 64-bit

word size, modulus with a first section of 74 bits and a second section of 54 bits, it

would have been obvious to select those particular numbers.

Lenstra and Hollmann are analogous art because they are in the same field of

endeavor of cryptology.

It would have been obvious to a person of ordinary skill in the art at the time of

the invention to modify Hollmann's device by selecting sections of a modulus to be of

certain sizes and the key size and the word size as described by Lenstra since they are

parameters that were used in the best-known cryptosystems (Lenstra, page 260,

section 2.2.1, lines 5-6).

Regarding claim **30**, Hollmann discloses "**Apparatus according to claim 18**" but

does not specifically disclose "**with means, for 256-bit ECC and 81 word size of 64-**

bit, the modulus comprises 81 first section of 202 bits and 81 second section of

54 bits."

However, Lenstra disclose key size of 256 bits and word size of 64 bits are well

known in cryptosystems and the key size and block size can vary (page 260, sec 2.2.1,

lines 5-13). Furthermore, a modulus with a first section of 202 bits and a second

section of 54 bits is an example of a combination of bits that is selected for an ECC

operation. Thus, barring any unexpected result from particular selection of 256-bit

ECC, 64-bit word size, modulus with a first section of 202 bits and a second section of

54 bits, it would have been obvious to select those particular numbers. Note that as

indicated in the rejection of claim **30** under *Claim Rejections - 35 USC § 112* above,

"81 word size of 64-bit", "81 first section of 202 bits" and "81 second section of 54 bits"

are considered as "a word size of 64-bit", "a first section of 202 bits" and "a second

section of 54 bits".

Lenstra and Hollmann are analogous art because they are in the same field of

endeavor of cryptology.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's device by selecting sections of a modulus to be of certain sizes and the key size and the word size as described by Lenstra since they are parameters that were used in the best-known cryptosystems (Lenstra, page 260, section 2.2.1, lines 5-6).

Conclusion

27.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRONG NGUYEN whose telephone number is (571)270-7312. The examiner can normally be reached on Monday through Thursday 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas Pham can be reached on (571)272-3689. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/T. N/

/Thomas K Pham/
Supervisory Patent Examiner, Art Unit 4148